

Security Assessment Agreement

This document aims to record the agreements between client, assessor and service provider about a specific security assessment and to make sure that all parties are aware of the contents of the test and the inherent risks of performing a test.

Typically this agreement is initially filled out by assessor and client and then discussed with the service provider before signing.

1 Parties

This section describes the parties involved in the security assessment. All of the below will be referred to as party (meaning a single party) or parties (meaning all three parties)

1.1 Client

The client is the party that has requested the assessor (see below) to perform a security assessment.

Company Name : _____
Address : _____
Postal code : _____
City : _____
Country : _____

1.2 Assessor

The assessor is the party that will perform the security assessment as requested by the client.

Company Name : _____
Address : _____
City : _____
Postal code : _____
Country : _____

1.3 Service Provider

The service provider hosts, maintains, manages and/or executes infrastructure or services related to the subject of the security assessment on behalf of the client.

Company Name : _____
Address : _____
Postal code : _____
City : _____
Country : _____

2 Scope

2.1 Subject/Area of the test

The security assessment to be performed is limited to the following subject (description of the test

target in business terms):

2.2 Timeframe

The assessment will be conducted in the following timeframe(s):

2.3 Addresses

The subject is identified by the following IP addresses and/or URL's:

2.4 Test activities

The following tests will be executed:

- External vulnerability assessment from the Internet
- Internal vulnerability assessment from the local network
- Application assessment
- Host configuration review

Other:

2.5 Denial of Service

The assessor **will/will not** knowingly execute tests of which it is known that they will render services provided by the subject unusable.

2.6 Social engineering

The assessor will/will not use social engineering during the assessment.

If social engineering is in scope, the target of this attack will be the client/the service provider/both the client and the service provider.

2.7 Alternation of data

The assessor will/will not attempt to alter data on any system in scope.

Client hereby gives explicit permission to do so and accepts the risk(s) of such alteration(s).

-or-

Data will only be altered after explicit permission of the client/the service provider/both the client and the service provider.

Data changes, for example in log files, in databases or on the filesystem, which are also caused by normal use/inspection of the systems (e.g. the alteration of access log files), cannot normally be avoided and are allowed.

3 Contractual arrangements

The relevant parties declare that the following contracts are in place:

- Client and assessor have a legally binding contract for the assessment.
- Client and service provider have a legally binding contract for the hosting, management, maintenance and/or execution of services included in the scope of the assessment.

4 Legal liability

Breaking into a computer system is not allowed by law. The assessment may include activities such as breaking security measures, producing false signals and/or keys or assuming a false identity.

However within the scope of the assessment, the assessor is performing activities on request of the client, therefore neither the client or the service provider or anybody on their behalf will hold the assessor liable or press legal and/or criminal charges.

Client and service provider will not hold the assessor liable for any damage to systems or service in scope as a result of the assessment and any third party claims of such nature.

The assessor understand that he may still be held liable for any of these activities outside the scope of the assessment or in case of gross neglect or abuse.

5 Risks

5.1 Operational impact

Even though all parties will do their best to prevent it, a security assessment may impact the confidentiality, integrity or availability of the subject.

The assessor advises both client and service provider to make sure that systems, services and or data can be satisfactory restored should this be necessary.

5.2 Project risks

A security assessment can potentially identify issues that due to their nature need to be addressed before deployment of the subject. Parties are aware that this may impact project timelines.

5.3 Completeness

The results from a security assessment are the indication of the security posture of the subject at the time of the test, they do not provide any guarantees for the future.

No security assessment can guarantee 100% security.

COTS and custom software often contains unknown (security) flaws that may not be discovered during the audit.

6 Practicalities

6.1 Support

The client requests the service provider to provide full cooperation to the assessment.

6.2 Contact persons

The following persons will act as the contact persons for the client (name, email, mobile phone):

-
-

The following persons will act as the contact persons for the assessor (name, email, mobile phone):

-
-

The following persons will act as the contact persons for the service provider (name, email, mobile phone):

-
-

6.3 Place of work

If the activities need to take place at a location of the client and/or service provider the relevant party/parties will make sure that:

- a suitable workplace is available.
- the assessor has access to the facility
- networks that are part of the assessment are available at the workplace if needed
- the assessor is allowed to connect their test equipment to these networks if needed

6.4 Test systems used

In case of an external assessment (from the Internet) the following addresses and domains will be used:

6.5 Change control

Any changes to the subject during the assessment will impact the accuracy of the assessment. Significant changes will only be performed after consultation with the assessor.

6.6 Reporting

Any critical issues found during the test will be communicated immediately with the contact persons of the client/service provider/client and the service provider.

The assessor will send the first draft of the report to the client/service provider/client and service provider.

This first draft will be discussed with the client/service provider/client and service provider prior to release of the final version.

The final version will be distributed to the client/service provider/client and service provider.

The copyright of the distributed materials rests with the client/service provider/assessor.

The assessor will/will not transfer the full rights to use the report to the client/service provider/client and service provider.

The distributed materials will be/will not be protected with electronic copy protection measures. Examples of these measures are Digital Rights Management, blocking of printing, blocking of the clipboard or substitution of fonts.

7 Confidentiality

Disclosing party is the party that discloses confidential information.

Receiving party/parties are those parties receiving such information.

All information exchanged between the parties will be regarded confidential.

Receiving parties will not disclose confidential information to any person, firm, cooperation or any other entity for any reason whatsoever, provided however, that such party may disclose the Confidential Information on a need-to-know basis to its professional advisers and all staff, both support and management, employed by it or any of its subsidiary, affiliated or associate companies provided that such persons are bound by a similar duty of confidentiality.

The Receiving Party must protect the Confidential Information of the Disclosing Party using a reasonable degree of care.

The obligations pursuant to this agreement do not apply to any Confidential Information that:

- is lawfully in the possession of the Receiving Party prior to receipt from the Disclosing Party;
- is or becomes publicly known, otherwise than as a consequence of a breach of this agreement; or
- is received from a third party without breach of any other relevant confidentiality obligation.

The obligations in this agreement do not apply to disclosing Confidential Information either (i) to a third party pursuant to a written authorisation from the Disclosing Party; or (ii) to satisfy a requirement of, or demand by, a competent court of law or governmental, or regulatory body or listing authority.

8 Governing law

This agreement is governed by, and will be construed in accordance with Dutch law.

The parties submit to the non-exclusive jurisdiction of the courts of The Netherlands in relation to any legal actions or proceedings arising out of or in connection with this agreement.

Damages would not be an adequate remedy for any breach of this Agreement and the parties shall be entitled to the remedies of injunction, specific performance and other equitable relief for any threatened or actual breach of this Agreement and no proof of special damages shall be necessary for the enforcement of this Agreement.

9 Signatures

Executed by the parties:

Client

Company name : _____

Name : _____

Job Title/Position : _____

Signature : _____

Assessor

Company name : _____

Name : _____

Job Title/Position : _____

Signature : _____

Service Provider

Company name : _____

Name : _____

Job Title/Position : _____

Signature : _____